LISTING OF CLAIMS

1. (Currently Amended) From a user's browser, a secure method of image production in a web-based imaging environment, said method comprising the steps of:

accessing a destination web service;

downloading into said browser web content associated with said accessed destination web service;

downloading into said browser a public encryption key from said accessed destination web service;

retrieving image data under control of said browser;

encrypting said retrieved image data, wherein said downloaded public encryption key is utilized as part of said encrypting step;

choosing desired options represented by said destination web service through said web content;

creating a print job reflecting said desired options, said print job including said image data;

transmitting said encrypted image data to said accessed destination web service; and

decrypting said encrypted image data by said accessed destination web service, wherein a private encryption key counterpart of said public encryption key is utilized as part of said decrypting step, said private encryption key being accessible exclusively to said accessed destination web service.

2. (Original) The method of claim 1 wherein said retrieved image data is previously referenced to a composition associated with said user's identity.

3. (Original) The method of claim 1 wherein said accessed destination web service represents a production device.

4. (Original) The method of claim 3 wherein said production device is a printer.

5. (Original) The method of claim 1 wherein said retrieving comprises accessing said user's identity from said destination web service via said web content through an imaging extension.

6. (Original) The method of claim 1 wherein said retrieving comprises accessing a hard disk local to said web browser.

7. (Original) The method of claim 1 wherein said image data is contained in a PDF file.

8. (Canceled)

9. (Previously Presented) The method of claim ~~8~~ 1 wherein said options include an option to print securely, the option to print securely providing a secure transmission of data to said destination web service.

10. (Canceled)

11. (Original) The method of claim 1 wherein:

said encrypting comprises synthesizing a session key, encrypting said image data using said session key, and encrypting said session key using said public encryption key;

said transmitting further comprises transmitting said encrypted said session key to said destination web service; and

said decrypting comprises decrypting said session key using said private encryption key counterpart of said public encryption key and then using said decrypted said session key to decrypt said encrypted image data.

12. (Previously Presented) A computer for providing secure image production in a web-based imaging environment, said computer operable to:

access a destination web service;

download web content from said destination web service to a user's browser;

download a public encryption key from said destination web service to the user's browser;

encrypt imaging data using said public encryption key as part of encryption process;

transmit said encrypted imaging data to said destination web service; and

direct said destination web service to decrypt said encrypted imaging data using a private encryption key counterpart of said public encryption key as part of decryption process, said private encryption key being accessible exclusively to said destination web service.

13. (Original) The computer of claim 12 wherein said imaging data is previously referenced to a composition associated with a user's identity.

14. (Original) The computer of claim 12 wherein said destination web service represents a production device.

15. (Original) The computer of claim 14 further operable to direct said destination web service via said web content to select production options for producing said imaging data by said production device.

16. (Previously Presented) The computer of claim 15 wherein said production options include an option to produce securely, the option to print securely providing a secure transmission of data to said destination web service.

17. (Original) The computer of claim 12 further operable to:

synthesize a session key;

encrypt said image data using said session key;

encrypt said session key using said public encryption key;

transmit said encrypted session key to said destination web service; and

direct said destination web service to decrypt said encrypted session key using said private encryption key counterpart of said public encryption key and then to decrypt said encrypted image data using said decrypted session key.

18. (Previously Presented) A system for providing secure image production in a web-based imaging environment, said system comprising:

a user's browser operable to encrypt image data using a first encryption key as part of encryption process and to transmit said encrypted image data;

a destination web service representing a production device, said web service operable to download said first encryption key into said user's browser, said destination web service further operable to receive said transmitted encrypted image data and to decrypt said received encrypted image data using a private encryption key counterpart of said first encryption key as part of decryption process; and

a data path interconnecting said user's browser with said destination web service.

19. (Original) The system of claim 18 wherein said production device is a printer.

20. (Original) The system of claim 18 wherein said data path is selected from the group consisting of hard wired data paths and wireless data paths.

21. (Original) The system of claim 18 wherein said first encryption key is a public encryption key.

22. (Original) The system of claim 21 further comprising a session key, said session key being operable to encrypt said retrieved image data, to be encrypted using said public encryption key, and to be decrypted using said private encryption key counterpart of said public encryption key.